

MENU

SEARCH

INDEX

DETAIL

JAPANESE

1 / 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-308582

(43)Date of publication of application : 05.11.1999

(51)Int. CI.

H04N 7/08

H04N 7/081

H04H 1/00

H04L 9/14

H04N 7/167

(21)Application number : 10-115451 (71)Applicant : SONY CORP

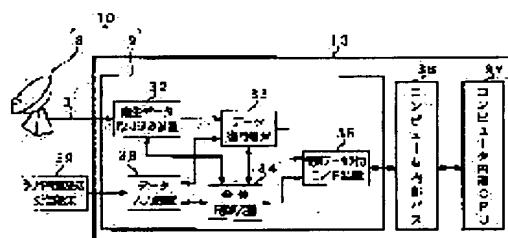
(22)Date of filing : 24.04.1998 (72)Inventor : ISHII MAKOTO

(54) DATA RECEIVER, ITS METHOD AND DATA TRANSMISSION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data receiver by which only a prescribed person can receiver data of a large capacity and many kinds of data simultaneously in the data transmission system where data with a large capacity are transferred through many channels and that utilizes a communication satellite.

SOLUTION: The data receiver 10 is provided with a reception antenna and a coaxial cable 31 that receive signal data distributed via a communication satellite, a satellite data acquisition device 32 that descrambles the signal data depending on the scrambling applied to the data and extracts a digital signal, a data decoder 33 having a data acquisition function that extracts prescribed data from the digital signal, a decoding function that decodes the digital data acquired by the data acquisition function by using an encryption key, and having a decoding key management function to manage the decoding key, and a received data output I/F device 35 that outputs the data decoded by the data decoder 33 externally.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's
decision of rejection][Kind of final disposal of application
other than the examiner's decision of

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-308582

(43)公開日 平成11年(1999)11月5日

(51)Int.Cl.⁶

識別記号

F I

H 0 4 N 7/08
7/081
H 0 4 H 1/00
H 0 4 L 9/14
H 0 4 N 7/167

H 0 4 N 7/08 Z
H 0 4 H 1/00 F
H 0 4 L 9/00 6 4 1
H 0 4 N 7/167 Z

審査請求 未請求 請求項の数16 O L (全 17 頁)

(21)出願番号 特願平10-115451

(22)出願日 平成10年(1998)4月24日

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 石井 眞

東京都品川区北品川6丁目7番35号 ソニー株式会社内

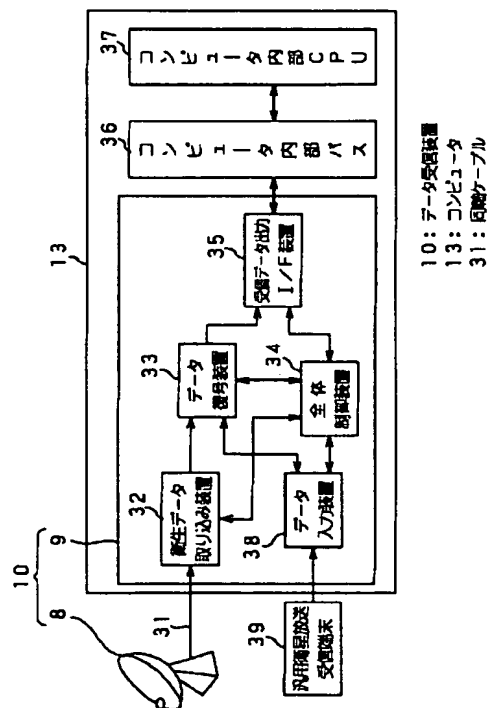
(74)代理人 弁理士 小池 晃 (外2名)

(54)【発明の名称】 データ受信装置及び方法、並びにデータ送信方法

(57)【要約】

【課題】 多チャンネル及び大容量でデータの転送を行通信衛星を利用したデータ伝送システムにおいて、所定の者のみが大容量のデータかつ多種類のデータを同時に受信することを可能にするデータ受信装置の提供を目的とする。

【解決手段】 データ受信装置10は、通信衛星を介して配信される信号データを受信する受信アンテナ8及び同軸ケーブル31と、上記信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出す衛星データ取り込み装置32と、上記ディジタル信号から所定のデータを取り出すデータ取得機能、当該データ取得機能により取得したディジタルデータを暗号鍵により復号する復号機能及び上記復号鍵を管理する復号鍵管理機能を有するデータ復号装置33と、データ復号装置により復号されたデータを外部に出力する受信データ出力 I/F 装置35とを備えている。



【特許請求の範囲】

【請求項 1】 衛星通信路を介して配信される信号データを受信するデータ受信装置において、

上記衛星通信路を介して配信される信号データを受信する受信手段と、

上記信号データに施されたスクランブル処理に応じてデスクランブルしてデジタル信号を取り出すデスクランブル手段と、

上記デジタル信号から所定のデータを取り出すデータ取得手段と、

上記データ取得手段により取得した暗号化されたデータを暗号鍵により復号する復号手段と、

上記暗号鍵を保管する暗号鍵保管手段と、

上記復号手段により復号されたデータを外部に出力する出力手段とを備えることを特徴とするデータ受信装置。

【請求項 2】 上記暗号鍵により復号される上記暗号化されたデータは、映像・音声データとともに伝送されるコンピュータのデータであることを特徴とする請求項 1 記載のデータ受信装置。

【請求項 3】 上記暗号化されたデータは、複数のパケットに分割されて配信されてきたデータであって、

上記復号手段は、実時間で上記各パケット毎に上記暗号化されたデータを復号することを特徴とする請求項 2 記載のデータ受信装置。

【請求項 4】 上記暗号鍵保管手段は、複数の暗号鍵を管理しており、

上記復号手段は、パケット毎に暗号鍵を交換して上記暗号化されたデータを復号することを特徴とする請求項 3 記載のデータ受信装置。

【請求項 5】 上記暗号鍵の選択は、データバスを介して外部から設定されることを特徴とする請求項 4 記載のデータ受信装置。

【請求項 6】 上記データ取得手段、復号手段及び出力手段は、一枚の基板上において構成されてなることを特徴とする請求項 1 記載のデータ受信装置。

【請求項 7】 上記出力手段は、データバスに接続されていることを特徴とする請求項 6 記載のデータ受信装置。

【請求項 8】 上記復号手段は、上記暗号化されたデータの復号に用いる所望の暗号鍵がないときには、当該復号対象としている暗号化されたデータが格納されているパケットを破棄することを特徴とする請求項 1 記載のデータ受信装置。

【請求項 9】 上記復号手段は、当該暗号化されたデータを送信した送信側が保持している暗号鍵と同じ上記暗号鍵保管手段において保管されている上記暗号鍵を用いて復号することを特徴とする請求項 8 記載のデータ受信装置。

【請求項 10】 上記復号鍵管理手段は、随時変更される可能性があるセッション鍵と、当該復号管理手段によ

り恒久的に管理されているマスター鍵の 2 種類の鍵を管理することを特徴とする請求項 1 記載のデータ受信装置。

【請求項 11】 上記復号手段は、ユーザからの設定により暗号方式を実時間で変更することが可能とされることを特徴とする請求項 1 記載のデータ受信装置。

【請求項 12】 上記衛星通信路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備え、

上記暗号化されたデータは、当該双方向データ伝送路を介して配信元に配信要求したデータからなることを特徴とする請求項 1 記載のデータ受信装置。

【請求項 13】 上記衛星通信路により伝送される衛星映像音声放送を受信する汎用の衛星映像音声放送用の受信端末を備えていることを特徴とする請求項 1 記載のデータ受信装置。

【請求項 14】 衛星通信路を介して配信される信号データを受信するデータ受信方法において、

上記衛星通信路を介して配信される信号データを受信する受信工程と、

上記信号データに施されたスクランブル処理に応じてデスクランブルしてデジタル信号を取り出すデスクランブル工程と、

上記デジタル信号から所定のデータを取り出すデータ取得工程と、

上記データ取得工程により取得した暗号化されたデータを、暗号鍵保管手段に保管されている暗号鍵により復号する復号工程と、

上記復号工程により復号されたデータを外部に出力する出力工程とを有することを特徴とするデータ受信方法。

【請求項 15】 スクランブル処理した映像音声情報を衛星通信路を介して配信するデータ送信装置において、上記衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加するデータ暗号化工程と、

上記暗号鍵を用いて暗号化されたデータ及び当該暗号化されたデータに付加されている配信先情報に対して、上記映像音声情報をスクランブル処理するのと同じ処理によりスクランブル処理を行うスクランブル処理工程と、

上記スクランブル処理された各種データを上記衛星通信路上に伝送するデータ伝送工程とを有することを特徴とするデータ送信方法。

【請求項 16】 上記暗号鍵を用いて暗号化されたデータ及び当該暗号化されたデータに付加されている配信先情報を複数のパケットに分割してから上記スクランブル処理手段により、スクランブル処理が施されることを特徴とする請求項 15 記載のデータ送信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、衛星通信路を利用

してデータの送受信を可能にするデータ受信装置及び方法、並びにデータ送信方法に関する。

【0002】

【従来の技術】近年、動画像等の圧縮技術により、例えば、現行放送やHDTV、AV機器などにおいて画像等の符号化方式に採用されているMPEG2 (Moving Picture Experts Group Phase 2) は、従来のアナログ放送に比べてデジタルによる多チャンネル化とチャンネル当たりのコストの削減をもたらしている。そして、このことは、映像・音声のみならずデータ放送等のサービスも可能にするといえる。そして、MPEG2方式による放送は、通信衛星を利用した多チャンネルデジタル放送としても採用されており、益々一般的になりつつある。

【0003】例えば、上記多チャンネルデジタル放送においては、衛星の高速転送スピード、例えば27MHzトランスポンダの場合、最大30Mbps、を生かした各種のデータ放送が実施されている。ここで、データ放送には、例えば音楽サービス、ゲームサービス、雑誌情報サービス、インターネット(WWW)サービスなどがある。

【0004】

【発明が解決しようとする課題】ところで、上述のような通信衛星を用いて配信されるデータを、所定の者、例えば、契約者のみに受信させることが提案されている。このようなデータの配信方法は、例えばデータ提供者が契約者のみにデータを送信したいとき、又は受信側のユーザが固有の情報として配信してもらいたいときなどに採用されると考えられるが、この場合、個人レベルでの秘密保持機構が必ず必要になる。

【0005】また、個人レベルの秘密を保持してデータを配信する手段として、配信データ暗号化が挙げられるが、通信衛星を利用することを考慮した場合には、最速30Mbpsの高速データ転送とされることから受信側において受信中のデータを、実時間かつ高速に暗号化されたデータを復号しなければならない。

【0006】さらには、上記秘密保持されているデータが同時刻に複数(例えば、複数種類、複数番組)受信しなければならないような状況も生じると考えられ、このような場合であっても、実時間で復号するような機構が必要となる。

【0007】なお、上述したように、各種データ放送サービスにより配信されるデータを受信するには、復号機能等の各種機能が要求されると考えられるが、同一のハードウェアで当該要求される処理を行うことが当該要求に耐え、効率よくデータの処理を行い得るデータ受信装置を提供することになるといえる。

【0008】また、今後サービス開始するであろう様々なデータ放送またはデータ通信サービスに汎用的に対応すること、例えば、現行及び今後の汎用的受信端末(I

RD: Interactive Receiver Decoder) との接続も容易に行えるようにすることなども重要である。

【0009】本発明は、上述の実情に鑑みてなされたものであって、多チャンネル及び大容量でデータの転送を行通信衛星を利用したデータ伝送システムにおいて、所定の者のみが大容量のデータかつ多種類のデータを同時に受信することを可能にするデータ受信装置及び方法、並びにデータ送信方法の提供を目的とする。

【0010】

10 【課題を解決するための手段】本発明に係るデータ受信装置は、上述の課題を解決するために、衛星通信路を介して配信される信号データを受信する受信手段と、信号データに施されたスクランブル処理に応じてデスクランブルしてデジタル信号を取り出すデスクランブル手段と、デジタル信号から所定のデータを取り出すデータ取得手段と、データ取得手段により取得した暗号化されたデータを暗号鍵により復号する復号手段と、暗号鍵を保管する暗号鍵保管手段と、復号手段により復号されたデータを外部に出力する出力手段とを備える。

20 【0011】このような構成を有するデータ受信装置は、受信手段により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル手段によりデスクランブル処理を施し、デジタルデータにして取り出し、そして、当該デジタルデータから、データ取得手段により、所定のデータを取り出す。

30 【0012】そして、データ受信装置は、データ取得手段により取得した暗号化されているデータを、復号手段により暗号鍵を用いて復号する。さらに、データ受信装置は、このように復号した得たデータを出力手段により外部に出力する。

【0013】これにより、データ受信装置は、スクランブル処理されて伝送されてくる信号から当該データ受信装置に宛てて送信された情報のみを意味のある情報として取り込むことができる。

【0014】本発明に係るデータ受信方法は、上述の課題を解決するために、衛星通信路を介して配信される信号データを受信する受信工程と、信号データに施されたスクランブル処理に応じてデスクランブルしてデジタル信号を取り出すデスクランブル工程と、デジタル信号から所定のデータを取り出すデータ取得工程と、データ取得工程により取得した暗号化されたデータを、暗号鍵保管手段に保管されている暗号鍵により復号する復号工程と、復号工程により復号されたデータを外部に出力する出力工程とを有する。

40 【0015】このデータ受信方法は、受信工程により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル工程によりデスクランブル処理を施し、デジタルデータにして取り出し、そして、当該デジタルデータから、データ取得工程により、所定のデータを取り出す。

【0016】そして、データ受信方法は、データ取得工程により取得した暗号化されているデータを、復号工程により暗号鍵を用いて復号する。さらに、データ受信装置は、このように復号した得たデータを出力工程により外部に出力する。

【0017】このデータ受信方法により、スクランブル処理されて伝送されてくる信号からデータ受信装置に宛てて送信された情報のみを意味のある情報として取り込むことができる。

【0018】また、本発明に係るデータ送信方法は、上述の課題を解決するために、衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加するデータ暗号化工程と、暗号鍵を用いて暗号化されたデータ及び当該暗号化されたデータに付加されている配信先情報に対して、映像音声情報をスクランブル処理するのと同一の処理によりスクランブル処理を行うスクランブル処理工程と、スクランブル処理された各種データを上記衛星通信路上に伝送するデータ伝送工程とを有する。

【0019】このデータ送信方法は、データ暗号化工程により、衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加し、スクランブル処理工程により、当該データ及び情報に、映像音声情報のスクランブルに使用されるスクランブル処理を施し、データ伝送工程により、このスクランブル処理されたデータを上記衛星通信路上に伝送する。

【0020】このデータ送信方法によりデータが配信されるデータ受信側では、スクランブル処理されて伝送されてくる信号から暗号化されている情報を上記宛先情報に基づいて取り出し、当該取り出した暗号化されているデータを暗号鍵により復号する。

【0021】

【発明の実施の形態】以下、本発明に係るデータ受信装置について実施の形態について図面を用いて詳しく説明する。この実施の形態は、通信衛星を利用してテレビジョン放送等を行う、いわゆるブロードキャスト型のデータ伝送システムにおいて、当該テレビジョン放送とともに配信されるデータを受信することができるデータ受信装置に適用したものである。

【0022】上記データ伝送システムは、図1に示すように、当該データ伝送システム1において契約者4に配信するデータを提供する情報提供者2と、情報提供者2から提供されたデータを所定の契約者4に送信する伝送路提供事業者であるサービス運用会社3と、上記サービス運用会社3との契約により当該サービス運用会社3からデータが配信される各契約者4A、4B、・・・、4Nが所有するデータ受信装置10と、上記サービス運用会社3から契約者4へのデータの転送に用いられる通信衛星5並びに公衆電話回線及び専用線等の有線通信路1

0と、各種情報を提供するとされるインターネット7とから構成される。このような形態とされるデータ伝送システム1は、例えば、現行のCSデジタル衛星放送と基本的には同様なシステム構成とされる。

【0023】このように構成されているデータ伝送システム1において、契約者4A、4B、・・・、4Nは、インターネット等において要求した情報の通信衛星5を介して配信するサービスが受けられる。

【0024】上記情報提供者2は、契約を結んだ契約者4に対して各種データを提供するものあって、例えば、各種情報を保有している複数の情報提供者2a、2b、・・・、2zから構成されている。この各情報提供者2a、2b、・・・、2zは、契約者4A、4B、・・・、4Nが要求した情報をサービス運用会社3により、当該情報要求した契約者4に配信する。

【0025】上記インターネット7は、各種情報をいわゆる公衆電話回線等の通信回線を介して提供しているものであって、上記契約者4A、4B、・・・、4Nが上記サービス運用会社3との契約によりアクセス可能とされる情報提供サービスである。例えば、インターネットにより、新聞情報、雑誌情報、音楽情報、ショッピング情報、インターネットWWW (World Wide Web) 情報等が契約者4A、4B、・・・、4Nに提供され、契約者4A、4B、・・・、4Nは、コンピュータ等でインターネット上の各種情報を閲覧及び操作可能とされる。

【0026】上記サービス運用会社3は、各情報提供者2a、2b、・・・、2zが取り扱い及び発信する様々な情報を取りまとめ、通信衛星5又は有線通信路6を介して契約者7に情報を配信している。このサービス運用会社3は、送信アンテナ12を備え、これにより、通信衛星5へのデータの伝送を行っている。上記通信衛星5を介することにより、サービス運用会社3は、一方向であるが大容量のデータの配信が可能になり、例えば30Mbpsの高速のデータ転送によるデータの転送が可能とされる。一方、サービス運用会社3は、有線通信路6を介することにより、契約者4A、4B、・・・、4Nとの間で双方向でデータの送受信を行うことができるものの、上記通信衛星5を利用したものよりも小容量のデータ転送に留まる。

【0027】ここで、上記サービス運用会社3は、上記通信衛星5を経由されて上記取りまとめた各種情報を契約者4A、4B、・・・、4Nに配信する際には、衛星通信路5上におけるデータフォーマットを、サービス運用会社3の自由なフォーマットとしているのではなく、衛星テレビ放送に用いられていると同様なフォーマットを採用している。例えば、サービス運用会社3は、欧州や日本等で運営されている衛星放送に採用されている現行のDVB (Digital Video Broadcasting) 規格等の標準規格に準じたフォーマットに変換して、上記情報提供者2等から取りまとめた各種情報を上記通信衛星5に

伝送している。上記契約者4 A, 4 B, . . . , 4 N は、コンピュータ13に内蔵してデータ受信装置を有している。例えば、各契約者4 A, 4 B, . . . , 4 N は、上記サービス運用会社3を契約した際に、上記データ受信装置の提供を受ける。

【0028】本発明の実施の形態とれる上記データ受信装置は、図2に示すように、衛星通信上に伝送された信号を受信するための受信アンテナ8と、受信アンテナ8により受信された信号を処理する信号処理部9とから構成されている。このデータ受信装置10は、例えば現行のBSテレビジョン放送やCSテレビジョン放送等において配信対象とされている映像や音声サービスのみならず、コンピュータ13が扱うことができる情報を受信することが可能となるように構成されている。データ受信装置10は、例えば現在一般的に普及されているコンピュータに内蔵するボードタイプとして構成され、受信アンテナ8からの同軸ケーブル31がコンピュータ13に内蔵された信号処理部9と接続されるような構造とされている。

【0029】このような構成を有するデータ伝送システム1においては、上述したように、上記契約者4は、上記サービス運用会社3によりインターネット7のWWW情報が閲覧可能とされており、これにより、上記契約者4 A, 4 B, . . . , 4 Nは、当該インターネット7上に存在する各種情報の配信を要求する等のインタラクティブなサービスの提供を受けることができる。すなわち、データ伝送システム1は、通信衛星5の使用用途を現行のBSテレビジョン放送またはCSテレビジョン放送用以外にも上記インタラクティブなサービスを可能にするように構成されているシステムである。これにより、契約者4は、インターネット10を閲覧して、欲しい情報があった場合、当該情報を通信衛星5を介して取得することが可能になる。

【0030】例えば、このように通信衛星5を使用して個人が要求した情報を取得しようとする場合、有線通信路6におけるときと同様に秘密保持管理が当然要求される。すなわち、有線通信路6のように情報提供者と情報受信者（契約者）の双方向において、他の者にあっては、当該送受信の対象とされる情報が取得不可能又は意味がないような情報とされるような秘密保持管理が要求される。

【0031】すなわち、上述したように、通信衛星5を利用してデータの配信を行おうとすれば、例えば、ある時刻において通信衛星路上には、現行のBSテレビジョン放送等のように契約者4 A, 4 B, . . . , 4 Nのみが見ることができる情報とともに、その中の一人の契約者、例えば契約者4 A、のためだけの情報が送信されることが起こる。このような場合でも、通信衛星5からの上記BSテレビジョン放送を契約者4 A, 4 B, . . . , 4 Nの全員が受信可能とされる一方で、ある契約者

（個人又は団体）のみが自分が契約した情報提供者から提供された情報を受信可能とされるような秘密保持管理が要求される。すなわち、上記BSテレビジョン放送に関しては、契約者の全員4 A, 4 B, . . . , 4 Nが受信することを可能にしながら、契約者4 Aが配信要求した情報に関しては、契約者4 Aだけは当該配信された情報を意味のある情報として得ることができ、また、何ら当該情報を要求していない他の契約者である契約者4 B, . . . , 4 Nは当該配信されてくる情報を意味のない信号として受信し、永久に意味のある情報として得ることができないような秘密保持管理が要求される。

【0032】なお、契約者4からのリクエストにより行う情報の検索については、次のようになる。すなわち、契約者4 A, 4 B, . . . , 4 Nが、ある任意の時刻に、インターネット7上のWWW情報を閲覧して、その情報の内に欲しい情報があり、当該情報が欲しい場合に、データ受信装置10を内蔵したコンピュータからモデムやイーサネット等により有線通信路6を経由して、情報のリクエスト命令をサービス運用会社3に発信する。特定の契約者4からの特定の情報のリクエストを受けたサービス運用会社3は、その情報の種別によりインターネット7にアクセス又は情報提供者2にアクセスして契約者4からの特定のリクエストの情報を得る。そして、サービス運用会社3は、得た特定の情報をその契約者しか受信できない形態に情報を変換して通信衛星5へのデータ伝送を行う。

【0033】以上のように、従来のようにBSテレビジョン放送、及びリクエストにより、通信衛星5を介した契約者4への配信が行われる。次に、データ伝送システム1において衛星通信路上に打ち上げるための所定のデータフォーマットに基づいたデータ作成操作について、図3を用いて説明する。本例では、データ作成の操作を5段階にして説明する。なお、データフォーマットを、DVB (Digital Video Broadcasting) 規格として説明する。

【0034】まず、データ操作<1>として、情報提供者2からの情報21₁, . . . , 21_n, . . . , 21_{n+m}は、いわゆる素のデータの形でサービス運用会社3に配信される。ここで、情報提供者2からサービス運用会社3に配信される情報21₁, . . . , 21_n, . . . , 21_{n+m}は、上述したように、契約者4 A, 4 B, . . . , 4 Nのための情報、又はその内の一人の契約者がリクエストした情報である。すなわち、例えば、上述したように、契約者4 A, 4 B, . . . , 4 NのためのBSテレビジョン放送の映像情報又はその一の契約者がインターネットにリクエストした情報である。そして、サービス運用会社3は、付加情報として各契約者へ配信すべき情報を、情報提供者2又はインターネット7から得ることにより、情報提供者2から受け取った情報21₁, . . . , 21_n, . . . , 21_{n+m}がどの契約者宛て

の情報であるかを知ることができる。例えば、サービス運用会社3には、IP (Internet Protocol) で規格化して上記各種情報を配信をする。すなわち、IPパケットに上記情報 $21_1, \dots, 21_n, \dots, 21_{n+m}$ が格納され、そのIPパケットのヘッダ部（以下、IPヘッダ部という。）に、当該各情報が配信されるべき各契約者にアドレス情報が格納される。例えば、IPヘッダ部は、図4に示すように、IPアドレス74に配信先のアドレスを格納し、IPアドレス73に配信元のアドレスを格納している。

【0035】次に、データ操作<2>として、上記データ操作<1>により得た情報 $21_1, \dots, 21_n, \dots, 21_{n+m}$ を、衛星通信路上でのデータフォーマットとして規定されているMAC (Media Access Control) フレームに変換する。ここで、MACフレーム化することにより、通信衛星経路上でのデータの伝送制御が可能となる。このMACフレーム化により、伝送対象となる各情報 $21_1, \dots, 21_n, \dots, 21_{n+m}$ がデータパケットP_Dに格納され、このデータパケットP_Dに伝送制御情報が格納されるMACヘッダH_{MAC}が付加される。

【0036】ここで、上記各情報は、上述したように、宛先が予め決定されており、例えば、上記情報 21_1 は、契約者4Aが要求した情報であり、上記情報 21_n は、全契約者4A、4B、 \dots 、4Nが要求した情報であり、そして上記情報 21_{n+m} は、契約者4Bのための情報である。そして、上記データパケットP_Dは、ここで、暗号鍵による暗号化処理が施されている。すなわち、上記各情報 $21_1, \dots, 21_n, \dots, 21_{n+m}$ が暗号化処理される。暗号鍵による暗号化処理とは、所定の情報に対して暗号鍵を用いて暗号化することをいう。そして、この暗号鍵により暗号化処理された情報は、当該暗号鍵に対応した復号鍵により解除され、読み取ることが可能となる。ここで、上記復号鍵は、データ受信装置10により各契約者が保持しているものである。

【0037】すなわち、サービス運用会社3は、各契約者のみが持つ暗号鍵を保持し、情報提供者2から配信された所定の契約者のみに配信したい情報を、当該配信を要求している契約者が保持している復号鍵に対応される暗号鍵により暗号化している。契約者4Aのための上記情報 21_1 は、契約者4Aが保持している復号鍵に対応した暗号鍵を用いて暗号化処理を行い、また、全契約者4A、4B、 \dots 、4Nのための上記情報 21_n は、契約者4A、4B、 \dots 、4Nの全員が有している復号鍵に対応された暗号鍵を用いて暗号化処理を行い、そして、契約者4Bのための上記情報 21_{n+m} は、契約者4Bが有する復号鍵に対応された暗号鍵を用いて暗号化処理を行っている。

【0038】このように、情報を要求した契約者に応じ

て暗号鍵を使いわけることにより、各契約者が保持している上記復号鍵は互いに異なっていることから、一の契約者のための暗号鍵により暗号化され、配信される情報が他の契約者が保持している上記復号鍵では復号することができなくなる。なお、各契約者の復号鍵は、サービス運用会社3から伝送されるものであり、例えば、当該伝送を定期的に行うことにより、安全が図られている。

【0039】なお、上記MACヘッダH_{MAC}には、当該情報を伝送すべき契約者の宛先を示すアドレスや、暗号化がされているかどうかを示す制御コードが格納されている。このMACヘッダH_{MAC}は、暗号鍵による暗号化処理が施されない部分であって、受信側である各データ受信装置10では、復号鍵により復号化を要することなく、このMACヘッダH_{MAC}を参照して、自分宛てのデータかどうかを識別することになる。例えば、図5に示すように、MACヘッダ70は、8ビットのSSID (Server System ID) と、24ビットのUDB (User Depend Block) 1と、32ビットのUDB 2の計64ビットで構成されている。特に、MACヘッダ70のUDB 2には、上記IPヘッダ内に書かれた送信先IPアドレスと同様の配信先のIPアドレスが書き込まれる。このMACヘッダ70に格納されている配信先のIPアドレスにより、受信側では単にハードウェア的にそれを読み出すことで、自分宛のデータパケットであるか否かを知ることができる。

【0040】そして、データ操作<3>として、上記データ操作<2>によって生成されたMACフレームは、衛星通信路上に配信するためのMPEG 2 (Moving Picture Experts Group Phase 2) 規格によるデータストリーム化がなされる。このMPEG 2規格によるストリーム化により、MACフレーム $23_1, \dots, 23_n, \dots, 23_{n+m}$ には、MPEG 2ヘッダH_{MPEG}及びフッタFが付加される。

【0041】ここでのMPEG 2ストリーム $23_1, \dots, 23_n, \dots, 23_{n+m}$ は、例えばプライベートセクション (Private Section) と呼ばれるデータフォーマットによって規定されるデータストリームであって、MPEG 2により標準フォーマットが規定されるものである。そして、上記MPEG 2ヘッダH_{MPEG}は、サービス運用会社3のベンダーIDや一つのMPEG 2ストリームの長さ等の制御情報を格納している。また、上記フッタFは受信側で衛星通信路上で一部ビットの損失もなく正常に情報が配信されたかどうかを知るための制御コードであって、例えばCRC (Cyclic Redundancy Check) によって付加されるコードである。このCRCによるコードを付加することにより、受信側では、受信したMPEG 2ストリームを先頭からCRC計算を行い、当該ストリームの最後まででの計算結果が付加されているフッタFの値と一致したときにのみ、受信したMPEG 2ストリームが正常に受信できたと認識することができ

るようになる。

【0042】そして、データ操作<4>として、上記データ操作<3>により生成された各MPEG2ストリーム23₁、・・・、23_n、・・・、23_{n+m}を、衛星通信路上に配信するために、上記DVBの規定に従って、MPEG2によるTSパケット（トランスポートストリームパケット）化を行う。

【0043】上記TSパケット化により、各MPEG2ストリーム23₁、・・・、23_n、・・・、23_{n+m}は、複数のペイロードデータ部とされてTSパケットPrsに分割されて格納され、各TSパケットPrsには、4バイトのTSヘッダHrsが付加される。

【0044】ここで、上記TSパケットPrs及びTSヘッダHrsにより構成されるパケット24₁、24₂、24₃、・・・、24_{k-2}、24_{k-1}、24_kは、88バイトの固定長として構成され、ここでは、格納されるMPEG2ストリームが大きいため、複数のTSパケットとされている。

【0045】上記TSヘッダHrsには、当該ヘッダ以降続くデータのための制御データが格納されており、具体的には、当該ヘッダ以降続くデータがサービス運用会社3から配信された制御データ又は契約者4が要求した情報かの識別を示すコード、若しくはそのTSパケットPrsが分割されたMPEG2ストリームの先頭か途中かを示す制御コードが格納されている。なお、上述したように、TSヘッダHrsにより行うサービス運用会社3から配信された制御データか否かの識別は、サービス運用会社3が当該データを受信するデータ受信装置10に対して制御データを送ることがあるためである。

【0046】そして、データ操作5において、上記データ操作4で生成されたパケット24₁、24₂、24₃、・・・、24_{k-2}、24_{k-1}、24_kは、衛星通信路上に配信するために必要な変調、例えばQPSK（Quadrature PSK）変調、スクランブル処理等されたパケット25₁、25₂、25₃、・・・、25_{k-2}、25_{k-1}、25_kとして通信衛星5に伝送される。

【0047】以上のように、データ伝送システム1において所定のデータフォーマットに基づいたデータ作成操作が行われて、通信衛星5へのデータの伝送が行われる。

【0048】次に、上述のように生成されて、通信衛星5による衛星通信路上に伝送されたデータのデータ受信装置10側における処理について説明する。

【0049】上記データ受信装置10は、図2に示すように、上記通信衛星5を介して配信される信号データを受信する受信手段を構成する受信アンテナ8及び同軸ケーブル31と、前記受信手段を構成し、上記信号データに施されたスクランブル処理に応じてデスクランブルしてデジタル信号を取り出すデスクランブル機能を有する衛星データ取り込み装置32と、上記デジタル信号

から所定のデータを取り出すデータ取得機能、当該データ取得機能により取得したデジタルデータを暗号鍵により復号する復号機能及び上記復号鍵を管理する復号鍵管理機能を有するデータ復号装置33と、データ復号装置により復号されたデータを外部に出力する出力手段を構成する受信データ出力I/F装置35とを備えている。なお、ここで、衛星データ取り込み装置32、データ復号処理装置33、データ入力装置38、受信データ出力I/F装置35及び全体制御装置34により上記信号処理部9を構成している。

【0050】また、データ受信装置10は、汎用衛星放送受信端末39から出力される当該データ受信装置10とのインターフェースとされるデータ入力装置38と、当該データ受信装置10全体を制御する全体制御装置34とを備えている。

【0051】そして、データ受信装置10は、コンピュータ内部バス36に接続され、このコンピュータ内部バス36を介してコンピュータ内部CPU37との間で各種データの送受信を行っている。

【0052】ここで、データ受信装置10に接続されている上記汎用衛星放送受信端末39は、例えば上述したようにBSテレビジョン放送用の受信端末である。

【0053】以下、上記データ受信装置10を構成する各部について説明する。

【0054】上記受信アンテナ30は、衛星通信路上のデータを当該データ受信装置10に取り込むための受信手段を構成している。この受信アンテナ30により受信したデータは、上記同軸ケーブル31を介して当該データ受信装置10の本体に入力される。ここで、入力されたデータは、IF信号データであって、IF信号データには、各契約者に配信されるデータと同じ、すなわち、当該IF信号データを受信した契約者が要求した情報以外の情報も全て含まれている。例えば、IF信号データは、データ受信端末用の制御情報や、他契約者宛ての情報である。

【0055】上記衛星データ取り込み装置32は、入力されたIF信号データについて、TTL（Time to Live）レベルにデジタルデータ化する装置であって、AD変換や信号の同期取りなどのデジタル衛星放送受信のために必要不可欠な最低限の処理を行うように構成されている。この衛星データ取り込み装置32は、入力されてデータに対してデスクランブル処理を施し、上記TSパケットPrsからMPEG2ストリームを再構築し、MPEG2ストリームとされたデジタルデータとして出力する。このデータ取り込み装置32から出力された上記MPEG2ストリームは、上記データ復号装置33に入力される。

【0056】データ復号装置33は、入力されたMPEG2ストリームについて復号処理を行うように構成されている。このデータ復号装置33は、MPEG2ストリ

ームの中のMACアドレス（宛先アドレス）と、全体制御装置34によって指定されたMACアドレスとを比較し、その比較結果が一致し、かつそのストリームが暗号化されている場合に、当該MPEG2ストリームについて復号処理を行う。これに対し、データ復号装置33は、受信したばかりのMPEG2ストリーム内のMACアドレスと一致したものがなければその場で当該受信したMPEG2ストリームを破棄する。このデータ復号装置33は、実時間で暗号化されたデータの復号処理を行っており、これにより、大容量のデータを高速で復号することを実現している。

【0057】上記データ復号装置33により復号されたMPEG2ストリームは、そのヘッダとされるMPEG2ヘッダH_{MPEG}とMACヘッダH_{MAC}が取り除かれた段階で受信データ出力I/F装置35に出力される。

【0058】上記受信データ出力I/F装置35は、当該データ受信装置10とコンピュータ13とのインターフェースとして構成されている。この受信データ出力I/F装置35は、正常に復号できたデータパケットをコンピュータ内部バス36に出力する。なお、受信データ出力I/F装置35は、そのデータ受信装置10を内蔵しているコンピュータ内部バス36のプロトコルを守るロジックを持っている。

【0059】上記全体制御装置34は、データ受信装置10の全体を監視及び管理するように構成されている。例えば、具体的には、データ受信装置10が接続されるコンピュータ13のアプリケーションからの制御命令や受信したデータの中に入っているデータ受信装置10の制御用のデータを解釈して、データ受信装置10全体の監視及び管理を行う。

【0060】上記汎用衛星放送受信端末39は、例えば衛星テレビジョン放送用の受信端末であって、例えば、現存するBSテレビジョン放送やCSテレビジョン放送等に用いられるものである。上述したように、サービス運用会社3は、上記BSテレビジョン放送等とともに情報提供者2から配信された各種情報を加工したデータとして衛星通信路上に伝送しており、汎用衛星放送用受信端末39は、上記BSテレビジョン放送と、当該BSテレビジョン放送とともに伝送されるデータをも入力されるように構成されている。

【0061】そして、データ受信装置10は、上記汎用衛星放送受信端末39とのインターフェースとして図示しない接続I/Fを持っており、これにより、接続される上記汎用衛星放送受信端末39からデータの入力が可能とされている。

【0062】このように、上記汎用衛星放送受信端末39とのインターフェースとして上記接続I/Fを持つことにより、データ受信装置10は、上記受信アンテナ8等を有していない場合であっても、上記汎用衛星放送受信端末39からデータの入力を可能とし、将来的な汎用

性を持つことができる。なお、この場合、上述したように上記衛星データ取り込み装置32からデータ復号装置33へのデータの出力がなくなり、データ入力装置38からデータがデータ復号装置33に入力されることになる。

【0063】上記データ受信装置10については、詳しくは、図6に示すように構成されている。この図6に示すデータ受信装置10を用いて受信されてデータの処理について詳しく説明する。なお、ここでは、契約者4Aにおけるデータの受信について説明する。

【0064】上記受信アンテナ8により受信された受信IF信号データ101は、契約者4が要求した情報21₁, ..., 21_n, ..., 21_{n+m}と、それ以外のデータ、例えば上記BSテレビジョン放送とを構成するデータとからなり、例えば、データ受信装置10の制御用情報や、他契約者宛ての情報も含まれているデータである。ここで、IF信号データは、上記図7に示すデータ操作<6>に示すように、スクランブル処理されたパケット25₁, 25₂, 25₃, ..., 25_{k-2}, 25_{k-1}, 25_kとされる。

【0065】このIF信号データ101は、上記衛星データ取り込み装置34によって、AD変換、信号の同期取りデスクランブル処理等の、デジタル衛星放送受信のために必要不可欠な最低限の処理が施され、最終的にTSパケット102として出力され、MPEG2ストリーム回復装置51に入力される。すなわち、ここでは、上記図7に示すように、データ操作<7>として、パケット24₁, 24₂, 24₃, ..., 24_{k-2}, 24_{k-1}, 24_kのスクランブル処理を行う。

【0066】上記MPEG2ストリーム回復装置51は、送信側においてTSパケット102として分割されたMPEG2ストリームの回復作業を行うように構成されている。このMPEG2ストリーム回復装置51が行うMPEG2ストリームの回復作業は、TSパケット102の先頭のTSヘッダH_{TS}内の制御コードを参照することにより、分割されているMPEG2ストリームの先頭を検出して、一つのMPEG2ストリーム103を生成している。すなわち、上記図7に示すように、データ操作<8>として、MPEG2ストリーム23₁, ..., 23_n, ..., 23_{n+m}を生成する。このMPEG2ストリーム回復装置51により回復されたMPEG2ストリーム103は、MPEG2ストリーム検査装置52に入力される。

【0067】MPEG2ストリーム検査装置52は、MPEG2ストリーム102に衛星通信路上でのノイズが発生しているか否かを検査する作業と、MPEG2ストリーム102のフィルタリング（振り分け）作業と、大きく分けて2つの作業を行うように構成されている。

【0068】MPEG2ストリーム検査装置52において行う衛星通信路上でのノイズの発生の検査は、MPE

G2ストリーム103のフッタFに付随されたCRCの値を用いて行っている。すなわち、MPEG2ストリーム検査装置52は、入力されたMPEG2ストリーム103の先頭から最後までMPEG2により規定されているCRCの計算を施し、最後まで計算したCRCの値と、送信側においてMPEG2ストリーム103のフッタFに付随されたCRCの値を比較して、同等であった場合のみ、「エラーなく通信できたパケット」として判断する。ここで、判断処理がなされたMPEG2ストリーム104は、MPEG2ストリーム破棄装置53へ送られる。なお、ここで、CRCの計算は入力されたMPEG2ストリーム103の最後まで行われるので、判定が決まるまではデータ一時蓄積装置54に保管される。

【0069】MPEG2ストリーム破棄装置53は、CRCにより計算エラーが発生したMPEG2ストリームについて破棄処理を行うように構成されている。具体的には、MPEG2ストリーム検査装置52から送られてくるストリーム破棄命令106により、当該ストリーム破棄命令106に対応されるMPEG2ストリームの破棄を行う。そして、CRCの計算エラーにより破棄したMPEG2ストリームがあった事実は、破棄した旨として全体制御装置34に報告される。

【0070】また、MPEG2ストリーム検査装置52において行うMPEG2ストリームのフィルタリングは、MPEG2ストリーム回復装置51から送られたMPEG2ストリーム103が、データ受信装置10の所有者である契約者4Aが要求した情報か否かを審査して、必要ならば後段のMPEG2ストリーム破棄装置53に送り、不要であればその場でMPEG2ストリーム103の破棄の処理を行うように構成されている。

【0071】具体的には、MPEG2ストリーム検査装置52は、MPEG2ストリーム内のMACフレーム内のMACヘッダH_{MAC}に格納されている宛先アドレスと、全体制御装置34からセットされる当該データ受信装置10自身がその時刻で保有しているアドレスとを比較して、受信すべきMPEG2ストリームと判断された時のみ、そのMPEG2ストリームをMPEG2ストリーム破棄装置53に出力する。通常、自分が持つアドレスは同時に数種類であり、それ以外のアドレスを宛先とするMPEG2ストリームはMPEG2ストリーム検査装置52において破棄されることになる。

【0072】よって、上記MPEG2ストリーム検査装置52により行った上記2つの作業により破棄されなかったMPEG2ストリームは、エラーなく正常に自分宛てに伝送されてきたデータであり、すなわち、自分自身が受け取るべきストリームである。なお、全体制御装置34によってセットされる自分のアドレスは、時刻と共に変化する可能性がある。

【0073】上述のように、暗号化されていないMACヘッダH_{MAC}に格納されている宛先アドレスを確認する

ことにより、復号化するなどの無駄な処理を要しなくても当該MACヘッダH_{MAC}が付加されている情報が自己宛に送られてきた情報か否かを瞬時に判断することができるようになる。これは、以降に続いて入力されてくるMPEG2ストリームは遅滞なく処理するを可能にする。

【0074】なお、MPEG2ストリーム検査装置52は、入力されたMPEG2ストリーム103からヘッダH_{MPEG}及びフッタFを取り除いた形のMPEG2ストリーム104のデータとしてデータ一時蓄積装置54に出力している。すなわち、上記図2に示すように、データ操作9として、MPEG2ストリーム22₁, ..., 22_n, ..., 22_{n+m}としてデータ一時蓄積装置5に出力している。

【0075】そして、データ一時蓄積装置54から出力されて、MPEG2ストリーム破棄装置53において破棄されずに通過したフッタFなしのMPEG2ストリーム107は、復号鍵検索装置55に入力される。

【0076】復号鍵検索装置55は、入力されてきたMPEG2ストリーム107に対する暗号鍵を検索するように構成されている。具体的には、復号鍵検索装置55は、暗号化されたユーザのためのデータの先頭のヘッダ情報を見て復号に必要な復号鍵を、データパケット（かたまり）毎に実時間で検索及び設定する。すなわち、復号鍵検索装置55は、MPEG2ストリーム107内のMACヘッダH_{MAC}内の、暗号がかけられているかどうかを示す制御ビットを見て、入力されたばかりのMPEG2ストリーム107内の情報21₁, ..., 21_n, ..., 21_{n+m}に暗号処理が施されているか否かを判別し、これに基づいて、復号鍵保管部56における復号鍵の検索等を行う。

【0077】ここで、暗号処理が施されていないことを確認した場合には、後段の復号装置58に対して復号しない命令とともに当該暗号処理が施されていないMPEG2ストリームが復号鍵検索装置55から出力される。なお、復号装置58に出力されるMPEG2ストリームは、これまで付加されていたMPEG2ヘッダH_{MPEG}及びMACヘッダH_{MAC}が取り除かれ、素の状態とされた情報21₁, ..., 21_n, ..., 21_{n+m}のデータパケットP₀として出力される。すなわち、上記図2に示のデータ操作10に示すように、情報21₁, ..., 21_n, ..., 21_{n+m}によって構成されるデータパケットとして出力される。

【0078】また、暗号処理が施されていることを確認した場合には、復号鍵検索装置55は、MPEG2ストリーム107内のMACヘッダH_{MAC}内の宛先アドレスに基づいて、復号鍵保管部56に復号鍵の要求命令109を出す。

【0079】復号鍵保管部56は、ある時刻においてデータ受信装置10を保有する契約者が受信することが許

可されているデータを復号するための復号鍵を保管している。この復号鍵保管部56は、例えばメモリにより構成されている。

【0080】また、復号鍵保管部56は、複数の復号鍵を保管することも可能とされており、それらの復号鍵は、全体制御装置56により管理されている。この復号鍵保管部56は、上記復号鍵の要求命令109により、対応した復号鍵を復号鍵検索装置55に出力する。例えば、復号鍵保管部56には、随時変更される可能性があるセッション鍵及び恒久的に保管されるマスター鍵が少なくとも含まれている。

【0081】ここで、セッション鍵とは、特定のサービス運用会社から送信されて情報を復号するための復号鍵であり、さらに、通常は、日毎、時間毎、ファイル毎、サービス毎等に逐次変化するものとされている。また、上記マスター鍵は、例えば、データ受信装置固有の復号鍵であって、例えば、上記セッション鍵を復号するために使用される。よって、このような場合には、マスター鍵により先ずセッション鍵を復号してから、当該セッション鍵により上記暗号化された情報の復号を行う。このように行うことに、情報の秘密保持を向上させることができるようになる。

【0082】そして、復号鍵保管部56に保管される復号鍵は、鍵設定部57により設定される。例えば、鍵設定部57は、配信されてくる復号鍵を復号鍵保管部56にセットすることや、上記復号鍵保管部56に復号鍵を設定することができる。例えば、鍵設定部57は、配信されてくる復号鍵を、コンピュータ内部バス36から、受信データ出力I/F装置35を介して得ることができ、全体制御装置34の制御により、復号鍵保管部56にセットする。例えば、このようにして復号鍵保管部56にセットされる復号鍵は、上記セッション鍵である。また、鍵設定部57は、工場出荷時に入力されるID等に基づいて、復号鍵保管部56に鍵を設置することができる。例えば、このように工場出荷に設定される復号鍵は、上記マスター鍵の少なくとも一部として用いられる。

【0083】上記復号鍵検索装置55は、復号鍵保管部54から送られてきた復号鍵及び当該復号鍵により暗号処理が解除されるMPEG2ストリーム108を復号装置58に出力する。なお、復号鍵検索装置55から出力されるMPEG2ストリームは、これまで付加されていたMPEG2ヘッダH_{MPEG}及びMACヘッダH_{MAC}が取り除かれ、素の状態とされた情報21₁、・・・、21_n、・・・、21_{n+m}、すなわち、データパケットP₀の状態とされて、復号装置58に入力される。

【0084】なお、上記復号鍵検索装置55が受け取ったMPEG2ストリームとされたデータパケットP₀を復号するための復号鍵が上記復号鍵保管部56に存在しない場合には、復号鍵検索装置55は、そのMPEG2

ストリームについての復号は不可能であることから、そのMPEG2ストリームを破棄する。そして、このように復号鍵が保持していないことによりMPEG2ストリームの破棄を行って場合には、その旨を全体制御装置34に報告する。

【0085】復号装置58は、復号鍵検索装置55からの受け取った復号鍵により、当該復号鍵とともに入力されたデータパケットP₀の復号、すなわち暗号処理の解除を行うように構成されている。すなわち、復号装置58は、復号鍵により暗号化されているデータパケットP₀について復号を行い、これにより、上記図7のデータ操作<10>に示すように、契約者4A及び全契約者のために転送されてきた情報21₁及び情報21₂のみを得ることができる。

【0086】なお、上述したように、復号鍵検索装置55は、暗号化されていないデータパケットについても復号装置58に出力しており、よって、復号装置58は、そのようなデータパケットが入力された場合については、復号鍵による復号をする必要がないので、何ら復号処理を施さずにその当該入力されたデータパケットを後段の復号後処理部兼パケット破棄装置58に出力する。

【0087】また、復号装置58では、入力されるデータパケット毎に、逐一復号鍵の更新入力を受け取り処理することが可能な能力を持つ。これにより、ある契約者4が複数の復号鍵を同時刻に保有していたとしても、対応可能である。また、復号鍵検索装置55からの命令によって、復号装置58は、様々な初期値や複数の暗号モードをデータパケット毎に切り替えることが可能となる。

【0088】復号装置58は、復号が終了したデータパケット111又は復号をする必要がなかったデータパケット111を、後段の復号後処理部兼パケット破棄装置59に出力する。

【0089】なお、上述したように、暗号処理された情報を復号するための部分として復号鍵保管部56、復号鍵検索装置55及び復号装置58をハードウェアとして構成することにより、実時間で暗号された情報の復号処理を実現することができる。

【0090】復号後処理部兼パケット破棄装置59は、データパケット111が復号装置58において正しく復号できた否かを検査する。なお、データパケット111は、汎用のインターネット用のパケットとされるIPパケットであるが、復号後処理部兼パケット破棄装置59は、正しく復号できたか否かを検査を、IPパケットのヘッダにあるヘッダチェックサム等の計算をする等、IPパケット内部のコードを主に用いて行っている。

【0091】ここで、復号が正常に行われたことを確認した場合には、復号後処理部兼パケット破棄装置59は、当該データパケット112のみを後段のデータ一時蓄積装置60に出力する。また、復号が正常に行われた

なかったことを確認した場合には、復号後処理部兼パケット破棄装置59は、当該データパケットを破棄し、その旨を全体制御装置34に報告する。

【0092】データ一時蓄積装置60内に貯えられたデータパケット112は、上記受信データ出力I/F装置35を介して、コンピュータのコンピュータ内部バス36に入力される。

【0093】また、上記図2に示すデータ受信装置10のデータ入力装置38は、図6に示す汎用衛星放送受信端末接続I/F61と汎用衛星放送受信端末接続I/F62とから構成されている。ここで、汎用衛星放送受信端末接続I/F61は、いわゆるTTLによるデジタルデータのインターフェースであり、また、汎用衛星放送受信端末接続I/F62は、いわゆるIEEE1394によって規格されたインターフェースである。

【0094】そして、汎用衛星放送受信端末接続I/F61及び汎用衛星放送受信端末接続I/F62は、衛星データ取り込み装置32と同時に作動することがないように構成されている。これにより、データの受信は、受信アンテナ30を介した衛星データ取り込み装置32か、汎用衛星放送受信端末接続I/F61又は汎用衛星放送受信端末接続I/F62かのいずれか一方の装置により当該データ受信装置10に取り込まれることになる。すなわち、衛星データ取り込み装置32によりデータが取り込まれている最中にあっては、汎用衛星放送受信端末接続I/F61、62の作動はなく、そして、逆も同じとされている。例えば、図8で示すように、受信アンテナ70により受信されて衛星テレビジョン放送が同軸ケーブル71を介して汎用衛星放送受信端末39に入力された場合には、衛星データ取り込み装置32は作動しないことになる。

【0095】上記汎用衛星放送受信端末39は、多チャンネルのBSテレビジョン放送等のデジタル衛星放送を受信することができる受信端末であって、例えばIRDである。そして、上述したように、サービス運営会社3から伝送される情報を受信可能に構成されている。

【0096】ところで、上述したように通信衛星5を利用して各種データの配信を行うサービス運営会社3については、他に存在するような場合であっても、サービス運営会社間に関してまったく異質なのではなく、統一化が図られるのが現状である。このことは、ユーザが、上記IRDといった一つの汎用衛星放送受信端末39により複数のサービス運用会社3からの情報配信を受けることができる可能性を示唆している。よって、汎用衛星放送受信端末39により、データ受信装置10は、複数の送信先の異なるデータを受信することができるように構成が可能になる。このような場合に対応して、例えば、汎用衛星放送受信端末39に入力されたデータが当該汎用衛星放送受信端末39において何らかのデータの細工、例えばICカードによる1次課金を処理する等が

なされた後に、データ受信装置10に入力したいといったデータの配信形態が今後出てくる可能性も考えられる。

【0097】上記汎用衛星放送受信端末接続I/F61、62はこのような事態を解決するものであって、すなわち、データ受信装置10は、汎用衛星放送受信端末接続I/F61、62が汎用性を持つインターフェースとして構成されることにより、あらゆる形態で配信されてくるデータを受信することができるようになる。これにより、異なったサービス運営会社による一般の衛星放送と衛星データ放送/通信サービスの共存が可能になる。なお、データ受信装置10は、上述したように2種類の汎用衛星放送受信端末接続I/F61、62に限定されることはなく、数、インターフェースのプロトコルも適宜決定される。

【0098】なお、上記全体制御装置34は、上述したような制御を行う他に主に次のような機能を有している。

【0099】全体制御装置34は、データ受信装置10全体のリセット及びイニシャライズを行う機能を有している。

【0100】また、全体制御装置34は、データ受信装置10全体の状態監視と、その情報をコンピュータ内アプリケーションに報告する機能を有している。

【0101】さらに、全体制御装置34は、MPEG2ストリーム検査装置52へのMACアドレスの制御命令を行う。

【0102】そして、全体制御装置34は、復号鍵保管部56への復号鍵のセットをセット命令によって行う機能を有している。

【0103】また、全体制御装置34は、各部からのパケット破棄報告の受信と、コンピュータ内アプリケーションへのその破棄の報告を行う機能を有している。

【0104】さらに、全体制御装置34は、その他、データ受信装置10内のすべての作業を統括して管理するように構成されている。

【0105】以上のように、データ受信装置10は構成されている。このデータ受信装置10は、信号処理装置9を構成する各部を一つの基板上に形成している。これにより、データ受信装置10は、実時間でスイッチングする機能等により同一のハードウェアで効率よく各機能を実行させることが可能になる。

【0106】なお、上述したように、通信衛星5により配信されたデータを受信したデータ受信装置10が、当該受信したデータから所定の情報のみを取り出す処理については、図7を用いると、次のように説明することができる。

【0107】なお、基本的には、ここで説明するデータ処理の流れは、上記図3を用いてデータ操作<1>～データ操作<5>として上記説明した処理手順と逆にな

る。しかし、受信側でのデータ操作において注意すべき点は、データ操作<6>からデータ操作<10>に進むに従い、データ受信装置10を構成する各ブロックにおいてデータが欠落していく可能性があることである。すなわち、所定の契約者、ここでは例えば契約者4Aとは何ら関係のないデータが破棄されるということである。

【0108】すなわち、例えば、契約者4Aにとっては、自分が持つデータ受信装置10によって、受信した全ての衛星通信路上のデータの信号から次々と様々な要因でデータが破棄されていき、最終的に「正常に受信できた信号の中で、しかも契約者Aのみが本来受け取れるべき情報」のみが、契約者4Aにとって意味ある形となって受信される。具体的に、契約者4Aが受信した衛星通信路上の全ての情報の中で、破棄される可能性のあるデータとして以下の複数ケースが考えられる。

【0109】データ操作<6>においては、衛星通信路上においてノイズが乗り、受信したデータが正常に復調できない場合、ストリームは破棄される。

【0110】そして、データ操作<7>においては、TSヘッダH_{TS}内の、制御データか情報かを示す識別ビットによって、ある契約者が要求する情報のみが取り込まれ制御データの方は破棄される。なお、ここでは、制御データが破棄されるというよりもデータ受信装置10がある機能への命令として取り込まれた後に破棄されることが多いといえる。

【0111】さらに、データ操作<8>としては、MP EG2ストリームのMP EG2フックFにある各ストリームのCRCの計算結果が異なった場合、MP EG2ストリームがそのまま破棄される。例えば、ここでの破棄の原因は、衛星通信路上でノイズが乗ったためであると考えられる。

【0112】そして、データ操作<9>においては、他の契約者宛ての情報であるために、MACフレーム内のMACヘッダH_{MAC}内に、自分宛ての宛先のものが存在しないためにパケット又はストリームが破棄される。または、自分宛てのMACフレームであるが、システムが正常に動作していないなどの理由により、復号時に必要な復号鍵を保有していないため、又は、復号すべき鍵もあるが、データ受信装置内の復号装置もしくはその周辺装置の不具合により生じる可能性があるので、復号に失敗したなどの理由によりパケット又はストリームが破棄される。このようにデータ操作9において破棄される可能性があるパケットが一番多い。

【0113】上記データ受信装置10は、通信衛星5からのデータを受信し、復号鍵保管検索装置55が保管されている受信データ用の刻々変化する復号鍵を瞬時に検索し、復号装置58が実時間かつ高速に受信データを復号し、受信データ出力I/F装置35が高速にデータを外部に出力する等の、複数のブロックを同時に備え持つことにより、一人のユーザが本人のみ受信したい、又

は送り手側がある特定のユーザにのみ配信したい機密性が高く大容量で多種類の衛星受信データのあるユーザが実時間で同時に受信することが可能になる。さらに、データ受信装置10により、上記特徴と同時に、汎用データ入力用インタフェース部とされる汎用衛星放送受信端末接続I/F61、62を備えることにより、現行及び将来の多様な衛星放送サービスへの柔軟な対応が可能になる。

【0114】

10 【発明の効果】本発明に係るデータ受信装置は、受信手段により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル手段によりデスクランブル処理を施し、デジタルデータにして取り出し、そして、当該デジタルデータから、データ取得手段により、所定のデータを取り出すことができる。そして、データ受信装置は、データ取得手段により取得した暗号化されているデータを、復号手段により暗号鍵を用いて復号し、このように復号した得たデータを出力手段により外部に出力することができる。

20 【0115】これにより、データ受信装置は、多チャンネル及び大容量でデータの転送を通信衛星を利用したデータ伝送システムにおいて、スクランブル処理されて伝送されてくる信号を受信して、当該スクランブル処理されている信号をデスクランブルして得ることができるとともに、当該データ受信装置のみに宛てて配信された情報のみを意味のある情報として取り込むことができるようになる。

30 【0116】このデータ受信方法は、受信工程により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル工程によりデスクランブル処理を施し、デジタルデータにして取り出し、そして、当該デジタルデータから、データ取得工程により、所定のデータを取り出すことができる。そして、データ受信方法は、データ取得工程により取得した暗号化されているデータを、復号工程により暗号鍵を用いて復号し、このように復号した得たデータを出力工程により外部に出力することができる。

40 【0117】このデータ受信方法により、多チャンネル及び大容量でデータの転送を通信衛星を利用したデータ伝送システムにおいて、スクランブル処理されて伝送されてくる信号を受信して、当該スクランブル処理されている信号をデスクランブルして得ることができるとともに、当該データ受信装置のみに宛てて配信された情報のみを意味のある情報として取り込むことができるようになる。

50 【0118】また、本発明に係るデータ送信方法は、データ暗号化工程により、衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加し、スクランブル処理工程により、当該データ及び情報に、映像音声情報の

スクランブルに使用されるスクランブル処理を施し、データ伝送工程により、このスクランブル処理されたデータを上記衛星通信路上に伝送することができる。

【0119】このデータ送信方法により、データが配信されるデータ受信側では、スクランブル処理されて伝送されてくる信号から暗号化されている情報を上記宛先情報に基づいて取り出し、当該取り出した暗号化されているデータを暗号鍵により復号することができる。これにより、このデータ伝送方法は、多チャンネル及び大容量でデータの転送を通信衛星を利用したデータ伝送システムにおいて、スクランブル処理されて伝送されてくる信号を受信して、当該スクランブル処理されている信号をデスクランブルして得ることができるとともに、所定のデータ受信装置のみに宛てて配信された情報のみを意味のある情報として取り込むことを可能にする。

【図面の簡単な説明】

【図1】本発明の実施の形態とされるデータ受信装置を備えるデータ送信システムの構成を示す図である。

【図2】上記データ受信装置の構成を示すブロック回路図である。

【図3】上記データ送信システムにおいて、配信の対象とされるデータに施す暗号化処理及びスクランブル処理の説明のために用いた図である。

【図4】上記配信の対象とされるデータがIPパケットに格納された場合に、当該IPパケットに付加されるIPヘッダを示す図である。

【図5】上記IPパケットがMACフレーム化された場合に、上記IPヘッダの情報を格納するMACヘッダを示す図である。

10 【図6】上記データ受信装置のさらに詳しい構成を示すブロック回路図である。

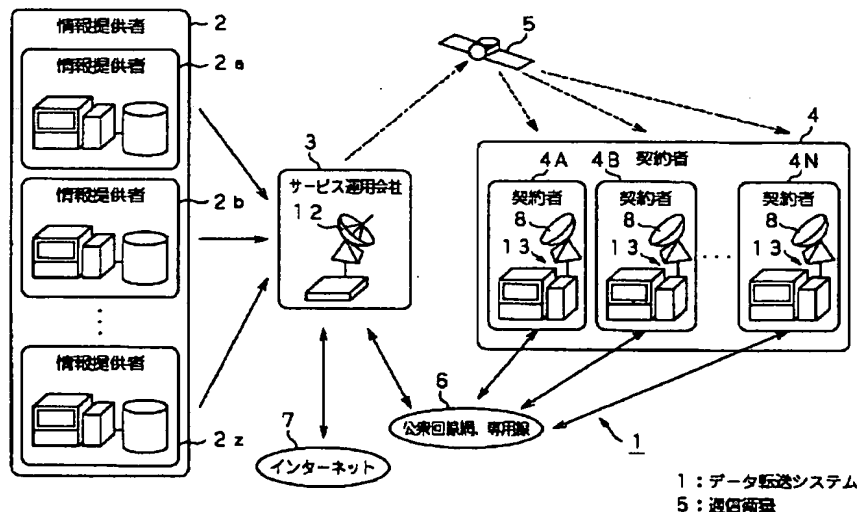
【図7】上記データ送信システムにおいて、配信されてくるデータに施すデスクランブル処理及び復号化処理の説明のために用いた図である。

【図8】上記データ受信装置の変形例を示すブロック回路図である。

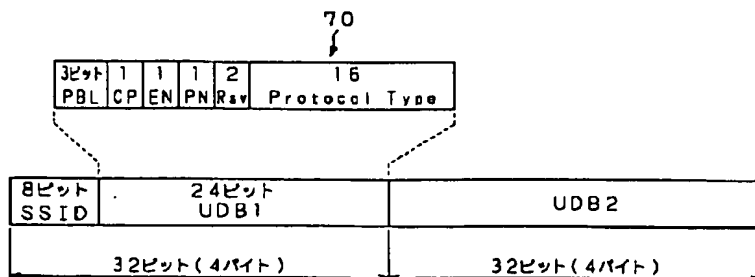
【符号の説明】

- 1 データ伝送システム、30 受信アンテナ、32 衛星データ取り込み装置、33 データ復号装置、35 受信データ出力I/F装置、38 データ入力装置

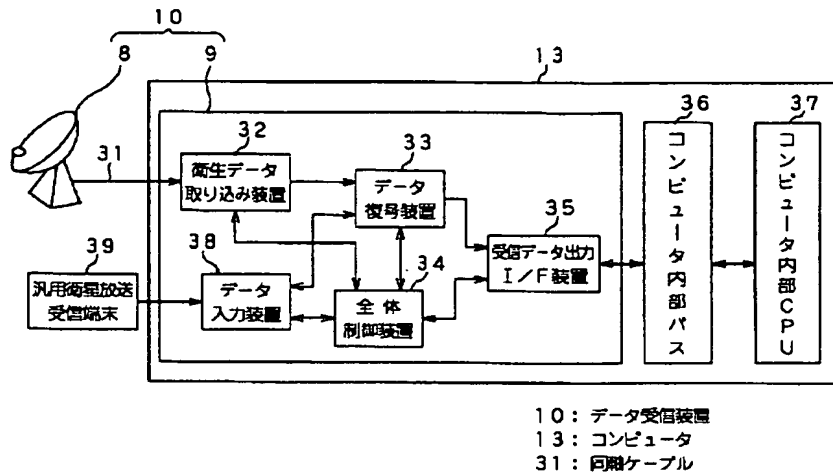
【図1】



【図5】



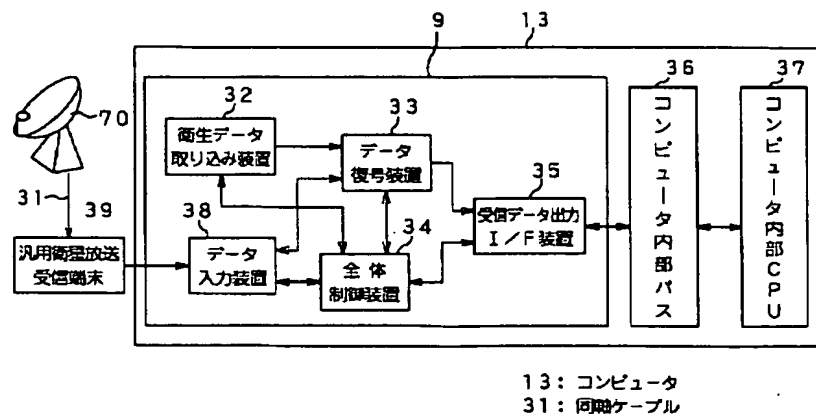
【図2】



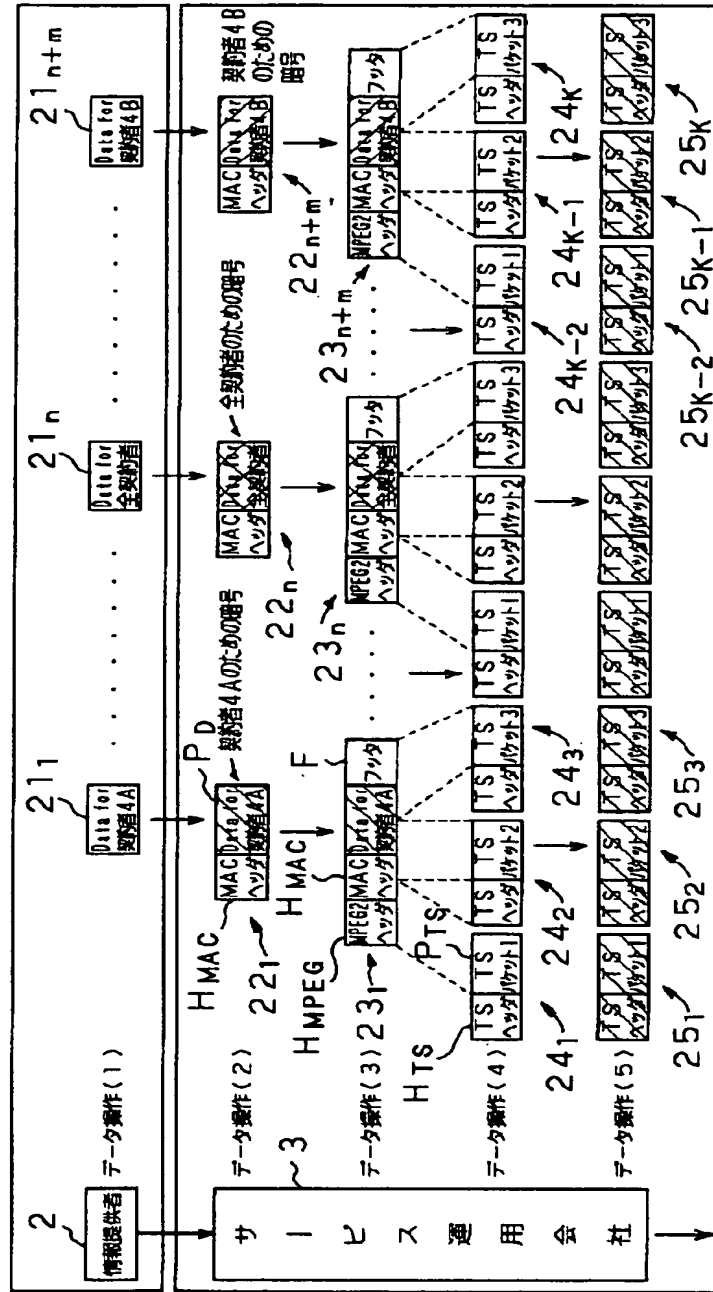
【図4】

0	4	8	16	31ビット
バージョン	IHL	TOS	Total Length	
Identification		フラグ	Fragment Offset	
TTL	Protocol	チェックサム		
送信元IPアドレス				73
送信先IPアドレス				74
オプション				

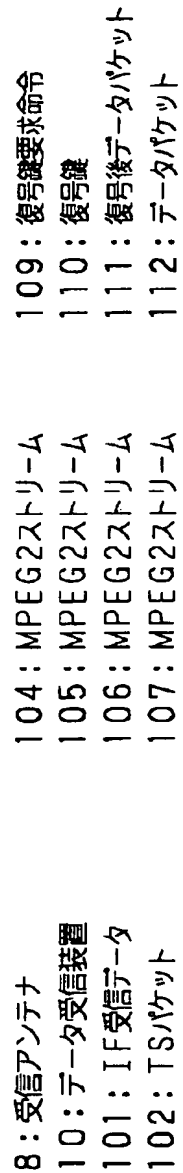
【図8】



【図3】



- 16 -



サービス運用会社から

通信衛星
↑

5. 五轴联动

